HADMÉRNÖK

KÖRNYEZETBIZTONSÁG

15. évfolyam (2020) 1. szám 91–105.
DOI: 10.32567/hm.2020.1.7

Legárd Ildikó[1]

Célpont vagy! – a közszolgálat felkészítése a kiberfenyegetésekre

You Are a Target! – The Preparation of the Public Administration against Cyber Security Threats

Napjainkban a közigazgatás megszervezése elképzelhetetlen infokommunikációs technológiák alkalmazása nélkül. Azonban bármennyire is védjük rendszereinket és a bennük tárolt adatokat a legmodernebb fizikai és logikai intézkedésekkel, még mindig a humán faktor jelenti a legnagyobb kockázatot. A fenyegetésekkel szembeni hatékony védelmet a felhasználók biztonságtudatossága tudja biztosítani, amely egy jól megszervezett és sikeres biztonságtudatosító program segítségével alakítható ki. A tanulmány bemutatja a humán alapú és a számítógép-alapú social engineering típusú támadás technikáit, áttekinti a biztonságtudatosság és az információbiztonság-tudatosító program fogalmát és ez utóbbi megvalósításának öt lépését, valamint megvizsgálja egy hatékony tudatosítóprogramhoz szükséges módszerek, kommunikációs csatornák és belső PR-eszközök alkalmazási lehetőségeit.

Kulcsszavak: információbiztonság, biztonságtudatosság, információbiztonság-tudatosító program, social engineering, belső PR-eszközök

Nowadays, the organisation of public administration is unimaginable without infocommunication technologies. Although the physical and logical protection of the system and the stored data may be well developed, the human factor will be a risk of security. The effective protection against the threats is to provide security awareness through implementing a well-developed and successful Information Security Awareness program.
This study presents the methods of human-based and IT-based social engineering attacks, reviews the category of security awareness and security awareness programs, determines five steps of the implementation and examines the different methods, the potential communication channels and internal PR tools of an effective program.

[1] Nemzeti Közszolgálati Egyetem Közigazgatás-tudományi Doktori Iskola, doktorandusz, e-mail: ildiko.legard@gmail.com, ORCID: https://orcid.org/0000-0002-1469-8679

Keywords: **information security, security awareness, security awareness program, social engineering, internal PR tools**

Bevezetés

Az utóbbi bő három évtizedben bekövetkező technológiai fejlődés, a digitalizáció ugrásszerű megnövekedése, az infokommunikációs eszközök és szolgáltatások rendkívüli fejlődése, az internet széles körű elterjedése, a gyors hozzáférés visszavonhatatlanul megváltoztatta az emberek életét, a vállalkozások működését és a közigazgatás szervezését.

Magyarországon a 2015-ben indított *Digitális Jólét Program* már alapvető célként határozza meg a digitális állam megteremtését és annak részeként a teljes közigazgatás digitális átalakítását [1].

A közigazgatás által döntően elektronikus információs rendszerekben[2] tárolt, feldolgozott és továbbított adatok és információk mennyiségének, illetve mibenlétének köszönhetően, napjainkban a magyar állami és önkormányzati szervek egyre több, a kibertér[3] felől érkező fenyegetésnek vannak kitéve, amelyek egyaránt érinthetik mind magukat a szerveket, mind pedig a munkavállalókat.

„Napjainkban jól elkülöníthető a kiberfenyegetések négy fajtája. Ezek a kiberbűnözés, a hacktivizmus és kiberterrorizmus, a kiberkémkedés és a kiberhadviselés" [2: 143–144.]. A közigazgatást érintő fenyegetések esetében mind a négy relevanciával bír.

Az NTT Security által 2019-ben közzétett *Global Threat Intelligence Report* alapján a közigazgatás a kiberfenyegetések 5 legnépszerűbb célpontja között van [3].

A közszférában dolgozók a támadók számára értékes és kiemelt célpontnak számítanak, hiszen általuk a nemzeti adatvagyon részét képző adatokhoz, információkhoz is hozzáférhetnek, vagy megbéníthatják egy egész szervezet és végső soron akár az egész ország működését is.

Ahogy Beláz Annamária fogalmaz tanulmányában, „Ahhoz, hogy a közigazgatási rendszer hosszútávon működőképes maradjon, valamint a rendszerekben előállított, tárolt, feldolgozott és továbbított adatok védelme biztosított legyen, az államnak elsőrendű feladata az információbiztonság szervezése és az információbiztonsági szemléletmód kialakítása, fenntartása" [4: 93.].

[2] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról 1 § (1) 14. b „elektronikus információs rendszer:
a) az elektronikus hírközlésről szóló törvény szerinti elektronikus hírközlő hálózat;
b) minden olyan eszköz vagy egymással összekapcsolt vagy kapcsolatban álló eszközök csoportja, amelyek közül egy vagy több valamely program alapján digitális adatok automatizált kezelését végzi; vagy
c) az a) és b) pontban szereplő elemek által működésük, használatuk, védelmük és karbantartásuk céljából tárolt, kezelt, visszakeresett vagy továbbított digitális adatok;"

[3] A kibertér egy globális tartomány az informatikai környezeten belül, amely tartalmazza az egymással összefüggő informatikai hálózatok infrastruktúráit, beleértve az internetet, a távközlési hálózatokat, a számítógépes rendszereket, valamint beágyazott processzorokat és vezérlőket [9: 30.].

Social engineering

Az elmúlt évtizedekben az információs rendszerek védelme egyre kifinomultabbá vált, ugyanakkor a rendszereket használók biztonságtudatossága nem tartott lépést a technikai fejlődés ütemével. Így nem meglepő, hogy a kiberbűnözők egy új és nagyon hamar népszerűvé vált támadási formát kezdtek el alkalmazni, az úgynevezett social engineering-et.

A social engineering az emberi hiszékenységre, együttműködő-képességre építő támadási forma. A támadók olyan alapvető emberi tulajdonságokat használnak ki, mint a segítőkészség, a hiszékenység, a befolyásolhatóság, a naivság vagy a kíváncsiság, amely jó eséllyel minden emberben ott lakozik, amelyekhez hozzáadódhat a biztonságtudatosság különböző okokból (alulképzettség, hanyagság stb.) bekövetkező hiánya, valamint a támadó általi szándékos megfélemlítés, zsarolás vagy megvesztegetés. Ezek kihasználásával már a támadó könnyen vagy mindenesetre könnyebben megkerülheti a rendszerek fizikai és logikai védelmi vonalát, például tűzfalakat vagy behatolás-detektáló rendszereket [5: 117.].

A social engineering típusú támadásokat, aszerint, hogy a támadó milyen módszereket használ, két csoportba lehet sorolni:

1. Humán alapú támadások [6], [7]

A humán alapú technikák alkalmazásához nem feltétlenül szükséges szaktudás, a támadó nem használ informatikai eszközöket, bárki által kivitelezhetők, azonban előzetes megfigyelést és felkészülést igényelnek. A támadó és áldozata között közvetlen kontaktust feltételez, így a lebukás veszélye is nagyobb [6: 4.].

Típusai:

- segítség kérése;
- segítség nyújtása (fordított social engineering);
- megszemélyesítés, vagyis az identitáslopás;
- thombstone theft, azaz a sírkőlopás, amely a megszemélyesítés egy speciális fajtája;
- shoulder surfing (képernyő lelesése);
- az irodai hulladék átvizsgálása, azaz a dumpster diving;
- tailgating, vagyis a szoros követés módszere a bejáraton történő bejutáshoz;
- piggybacking: a támadó az áldozat segítségével és tudtával jut át a bejáraton.

2. Számítógép-alapú támadások [8], [7]

A közvetett kapcsolattartást preferáló, számítógép-alapú támadások sokkal elterjedtebbek, mivel a támadó valamilyen informatikai eszközön keresztül lép kapcsolatba az áldozattal, így kisebb a lebukás veszélye.

Típusai:

- adathalászat – phishing: olyan üzenet, jellemzően e-mail, küldése az áldozatnak, amely megtéveszti őt és olyan hamis weboldalra „irányítja át", ahol kiadja személyes adatait, felhasználónevét, jelszavát. Több vállfaja ismert:
  - hamisított e-mailek és hamisított weboldalak (scam); vishing (VOIP-csalás), vagyis telefonos adathalászat; smishing, amelynek során az adathalász üzenet sms-ben érkezik; pharming, azaz az eltérítéses adathalászat; whaling, vagyis „bálnavadászat", amelyek esetében a célpontok köre a vezetői réteg; nyereményjátékokat, ajándékokat vagy ingyenes szolgáltatásokat hirdető áloldalak.
- kártékony programok: a támadás során olyan rosszindulatú kódok vannak elrejtve az eszközön vagy a fájlon, amelyeknek segítségével megszerezhetik a célszemély vagy egy szervezet adatait, például:
  - keylogger, azaz billentyűzetnaplózó; baiting: fertőzött, kártékony kódokat tartalmazó adathordozó eszköz (pendrive, CD, DVD, SD-kártya) „elvesztése" a kiszemelt szervezetnél vagy annak közelében, amit a gyanútlan és óvatlan alkalmazott csatlakoztat a saját gépéhez, így megfertőzve a saját, sőt jó eséllyel az egész szervezet rendszerét; javítás, frissítés felajánlása; trójai programok; veszélyes csatolmányok.
- Wi-Fi-hálózat veszélyei:
  - A hálózat üzemeltetője képes monitorozni a hálózaton zajló adatforgalmat, így elsősorban a nyílt hozzáférésű Wi-Fi-hálózatok rejtenek magukban veszélyeket, hiszen gyakran adathalász célokat szolgálnak, bár előfordulhat jelszóval védett hálózatok esetében is.
- okostelefon-alkalmazások általi hozzáférés – alkalmazásengedélyekből fakadó kockázatok: az okostelefonra telepített alkalmazások nemcsak a készülék alapvető funkcióihoz, hanem használatukért cserébe egyéb adatokhoz és információkhoz is kérnek és általában kapnak hozzáférést, mint például a felhasználó személyes adataihoz, névjegyeihez, fényképeihez, üzeneteihez.

A social engineering típusú támadás forgatókönyve – bár céljától függően más és más környezetben hajtják végre – általában állandó, és leggyakrabban négy lépésből áll, amelyeket egymásra épülve hajtanak végre. A lépések a következők [9: 52–54.]:

1. információszerzés: tipikusan internetről szerzett információk: közösségi hálózatok, keresőoldalak, a szervezet saját honlapja, telefonon keresztüli vagy írásban történő információszerzés, esetleg személyes felkeresés;
2. kapcsolat kiépítése a cél szempontjából legalkalmasabbnak ítélt és kiválasztott személlyel, aki akár egy vezető is lehet;
3. kapcsolat kihasználása;
4. támadás végrehajtása.

A social engineering típusú támadás alapja a támadás sikeres végrehajtásához szükséges információk megszerzése. Napjainkban az esetek döntő többségében a támadók az internet segítségével, online és elsősorban a közösségi oldalakról (például Facebook,

Twitter, LinkedIn) gyűjtik a szükséges információkat, mivel ezeken az oldalakon kis költséggel, gyorsan, nagy mennyiségű adat érhető el [10: 396.].

A személyre utaló információk megszerzése elősegíti a tökéletes célpont, a leggyengébb láncszem kiválasztását a szervezetnél, akin keresztül majd a támadók sikeresen férhetnek hozzá a kívánt rendszerhez.

„A social engineering típusú támadások sikeres végrehajtása két tényezőn múlik, egyrészt az informatikai eszközök és rendszerek sebezhetőségén, másrészt a felhasználók biztonságtudatossági ismeretein és azok megfelelő alkalmazásán, hiszen ha az alkalmazottak ismerik a lehetséges támadási és védekezési alternatívákat, akkor a különféle bizalmas információk megszerzésére irányuló támadások bekövetkezésének valószínűsége csökkenthető" [11: 269.].

Biztonságtudatosság (security awareness) és a biztonságtudatosító programok

Biztonságtudatosság

A biztonságtudatosságnak, pontosabban az információbiztonság-tudatosságnak (information security awareness) nincs egy általánosan elfogadott fogalma, annak összetevőit több magyar és nemzetközi kutatás is megkísérelte meghatározni.

Egyes szerzők a fogalom egyéni aspektusait hangsúlyozzák, minthogy a biztonságtudatos személy nemcsak a megfelelő szintű tudással rendelkezik az információbiztonság területén, hanem megérti és elfogadja annak jelentőségét, és képes az elsajátított ismereteknek megfelelően cselekedni és viselkedni [12], [13]. Aldawood és Skinner a felhasználó azon képességeit emeli ki, hogy képes felismerni, beazonosítani, elkerülni vagy megbénítani egy rosszindulatú támadási kísérletet [14: 6.].

Nemeslaki András és Sasvári Péter a definíció szervezeti aspektusait emeli ki, mint hogy „az információbiztonság-tudatosság a szervezet kultúrájának része, olyan gondolkodás- és magatartásmód, amely biztosítja, hogy a szervezetek alkalmazottai elkötelezettségből elismerik a biztonsági intézkedések jogosságát, betartják azokat, és másokkal is megismertetik, illetve betartatják ezeket" [15: 169.]. Bulgurcu és társai úgy határozzák meg az információbiztonság-tudatosságot, mint a munkavállaló általános ismereteinek és attitűdjének halmazát az információrendszerek használatával kapcsolatban úgy, ahogy azt a szervezeti környezetben értelmezik [16: 532.]. Az információbiztonság-tudatosság ebben a vonatkozásban két fő területből áll, egyrészt az általános szintű információbiztonsággal kapcsolatos tájékozottságból, másrészt az információbiztonsági szabályozások és stratégiák ismeretéből [17: 54.].

Az információbiztonság-tudatosság fogalmának alábbi, általános meghatározására teszek javaslatot:

Az információbiztonság-tudatosság a tudás, a képességek és a viselkedés olyan hármasa, amely biztosítja az egyén számára a megfelelő szintű informatikai és információbiztonsági ismereteket, az ezekre épülő és alkalmazásukat biztosító képességeket, valamint e két elemnek megfelelő, belső igényként megjelenő, az információbiztonság jelentőségét elismerő viselkedést.

Információbiztonság-tudatosító programok

A biztonságtudatosság fejlesztése kiemelt feladat az egyéneknél és szervezeteknél egyaránt, amelynek legfontosabb eszköze az információbiztonság-tudatosító programok kialakítása.

Számos nemzetközi informatikai biztonsági szabvány utal a tudatosítási programra, mint a minősítés megszerzésének előfeltételére, úgy mint az ISO 27001, COBIT, vagy az ISO 9001:2000 [12: 6.].

Szabályozás

A kiberbiztonságra vonatkozó magyarországi dokumentumokban, szabályozásban kiemelt figyelmet fordítanak a tudatosítás jelentőségének hangsúlyozására.

A 2013-ban elfogadott *Nemzeti Kiberbiztonsági Stratégia* a kiberbiztonság fogalmi elemeként határozza meg a tudatosságnövelő eszközök folyamatos és tervszerű alkalmazását [18].

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv.) kimondja, hogy az elektronikus információs rendszerek védelme érdekében a szervezet vezetője köteles gondoskodni „az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a szervezet munkatársai információbiztonsági ismereteinek szinten tartásáról" [19: 11. § (1) g)].

Az Ibtv. hatálya alá tartozó szervek számára a biztonságtudatosság képzésekkel kapcsolatban további feladatokat állapít meg a 41/2015. (VII. 15.) BM rendelet [20: 3.1.7.].

Az információbiztonság-tudatosító programok eredményessége

Számos hazai és külföldi kutatás megerősíti azt a tényt, hogy az alkalmazottak hiába vesznek részt egy tudatosító képzésen, hiába vannak birtokában a szükséges információbiztonsági tudásnak, szándékosan vagy nem szándékosan mellőzik vagy nem veszik figyelembe a biztonsági folyamatokat, előírásokat [17], [21], [22], [5]. Nemeslaki András és Sasvári Péter 2014-ben a magyar üzleti és közszféra információbiztonság-tudatosságát vizsgálta, és arra a megállapításra jutottak, hogy az információbiztonság-tudatosság fejlettnek mondható a közszférában az állami intézményeknél, valamint az állami tulajdonú szervezeteknél, mégis az alkalmazottak kisebb részénél még mindig fejlesztésre szorul [15].

Ezért a legfontosabb, hogy nem elegendő pusztán egy tudatosító programot megszervezni, hatékony és sikeres program szükséges ahhoz, hogy az alkalmazottak viselkedése pozitív irányban változzon.

A szakértők többsége egyetért abban, hogy a hatékonyság azt jelenti, hogy a biztonságtudatosító program képes a résztvevők tudását, attitűdjeit és viselkedését pozitív irányban változtatni az információbiztonság szempontjából, ezáltal csökkentve és megelőzve a szervezetre ható biztonsági fenyegetéseket és kockázatokat [23], [24: 63–64.].

Hogyan fejlesszünk hatékony és sikeres tudatosítási programot?

A következő öt lépésben bemutatom, hogyan lehet egy szervezeti igényekhez igazodó, ugyanakkor a felhasználóknak nemcsak a tudásbővítésre, hanem a képességeik fejlesztésére és viselkedésük megváltoztatására fókuszáló tudatosítási programot kialakítani.

1. A tervezéshez szükséges információk megszerzése:
   - a szervezet jellemzői: köz- vagy magánszféra, milyen típusú adatokat kezel, a szervezet stratégiája milyen hosszú- és rövidtávú célokat fogalmaz meg;
   - az információbiztonság szempontjából a kulcsterületek beazonosítása, ahol a biztonsági problémák jelentkeztek, a fenyegetések, kockázatok és incidensek tipizálása és ezek gyökereinek elemzése, valamint a szükséges helyreállító intézkedések beazonosítása;
   - a szervezet humán jellemzői: hány fős a szervezet, mekkora a fluktuáció; mely munkavállalói körnek szeretnénk a programot szervezni, az érintetti kör kor szerinti összetétele, munkaköreik és biztonságtudatosságuk szintjének meghatározása.
2. Felsővezetői támogatás biztosítása: kutatások igazolják, hogy a támogatás nélkülözhetetlen eleme a sikeres programnak [25].
3. A tudatosító program megtervezése:
   - a célcsoportnak megfelelő tudatosítóanyag összeállítása,
   - a szervezeti és humánpolitikai jellemzőkhöz igazodó módszerek és kommunikációs csatornák kiválasztása, valamint
   - az időzítés megtervezése.
4. A tudatosító program megvalósítása.
5. A program megvalósítása közben és végén a visszacsatolások alapján a program korrekciója.

A program sikeressége és hatékonysága szempontjából a 3. pont, tehát a tudatosító program megtervezése kulcsfontosságú tényező. Ahhoz, hogy a program képes legyen a résztvevők tudását, attitűdjeit és viselkedését megváltoztatni, szükséges, hogy a megfelelő embernek, a megfelelő információt, a megfelelő formában adjuk át.

A célcsoportnak megfelelő tudatosítóanyag összeállítása

A tananyag összeállítása szempontjából nagyon fontos tényező, mondjuk úgy, az „érzékenyítés". Egy szervezeten belül az egyik leggyakoribb probléma a veszélyérzet hiánya, amely a fenyegetettség fel nem ismerésén, valamint a munkatársak biztonsággal és a kapcsolódó védelmi intézkedésekkel való passzív viszonyán alapszik, ami kiegészül a biztonsággal kapcsolatos belső szabályozók nem megfelelő alkalmazásával vagy mellőzésével.

A tananyag összeállítása során a legfontosabb átadandó üzenetre kell koncentrálnunk, arra, hogy bárki áldozattá válhat ebben infokommunikációs technológiák és elektronikus információs rendszerek által átszőtt világban, viszont néhány nagyon

fontos tanács és trükk segítségével időben elkerülhetjük, hogy potenciális célponttá váljunk.

Tehát a program alapvető célja, hogy felhívja a figyelmet a potenciális fenyegetésekre, segítséget nyújtson a támadások időben történő felismeréséhez és elhárításához, valamint összességében hozzásegítse a résztvevőket elsősorban a munkahelyi, ugyanakkor a személyes és az otthoni biztonsághoz is. A cél elérése érdekében egyszerű, rövid, a napi gyakorlatban és a munkavégzés során jól alkalmazható tudást szükséges közvetíteni a résztvevők felé érdekes, újszerű formában.

A szervezeti és humánpolitikai jellemzőkhöz igazodó módszerek és kommunikációs csatornák kiválasztása

Az információbiztonsági tréningeknek számos formája ismert, amelyek különféle kommunikációs eszközökre építenek.

Aldawood és Skinner a tudatosítási programokról írt tanulmányukban, módszereit tekintve különbséget tesznek a tradicionális és a modern social engineering tréning és tudatosító program között. Meglátásuk szerint a hagyományos tréningek eszköztára – a belső vagy külső képzések, tréningek, poszterek, emlékeztetők és az online kurzusok – általában unalmas, fárasztó, nem tartják fenn a figyelmet, túl általánosak, formálisak és a tartalmat túl komoly környezetben közvetítik, valamint a módszerek egyáltalán nem alkalmazkodnak a résztvevők egyéni tanulási képességeihez. Ezek a tréningek egyszerűen csak elmondják a tudnivalókat a támadásokról, ugyanakkor nem mutatnak be valódi, megtörtént eseteket és nem adnak praktikus tanácsokat, hogy hogyan ismerjenek fel, illetve kezeljenek a résztvevők egy ilyen támadást. Tehát a tradicionális formák egyedüli alkalmazása nem biztosítja a megfelelő biztonsági kultúra kialakulását a résztvevőknél.

Ezzel szemben a modern tudatosító programok szimulációs technikákat, interaktív játékokat, virtuális laboratóriumokat, valamint tematikus videókat és modulokat alkalmaznak. A szimulációs technika például segít a social engineering módszerek tudatosításában, az interaktív játékok és virtuális laboratóriumok közreműködésével kipróbálható, hogy egy támadás azonosításától a kárenyhítésig milyen lépcsőkön keresztül vezet az út. Ezek a modern módszerek segítenek az alkalmazottaknak felismerni, hogy vajon egy üzenet támadás-e vagy sem. Ráadásul ezeket a gyakorlatokat az alkalmazottak a munkájuk mellett is egyszerűen elvégezhetik, így nem jelentenek plusz terhet számukra [14: 6–8.].

Szász Antónia és Kiss Gábor tanulmánya a jelszóvisszafejtő programok oktatási célú felhasználásáról alátámasztja a hagyományos és a modern eszközök közötti különbségtételt [26].

A legfrissebb nemzetközi kutatási eredmények mind kiemelik a tudatosítás szempontjából a megfelelő kommunikáció jelentőségét. A SANS Intézet által évente összeállított „Security Awareness Report" már 2017-ben a tudatosítási program sikerességének kritikus pontjaként emelte ki a megfelelő kommunikációt [27].

Ezért is nagyon fontos, hogy beazonosítsuk a célközönséget és igényeit, hogy a megfelelő kontextusban és megfelelő nyelvezettel tudjunk hozzájuk szólni.

E feladat megoldásában segítségül hívom a marketing, a marketingkommunikáció, valamint a PR fogalmát, és megvizsgálom e fogalmak és eszközrendszereik alkalmazási lehetőségeit az információbiztonság területén.

A marketing fogalmát sokan, sokféleképpen definiálták már, mégis a legelfogadottabb és leginkább idézett meghatározását Bauer András és Berács József közölték *Marketing* című könyvükben [28]. Eszerint szűkebb értelemben „a marketing olyan vállalati tevékenység, amely a vevők/felhasználók igényeinek kielégítése érdekében értelmezi a piacot, meghatározza az eladni kívánt termékeket és szolgáltatásokat, megismerteti azokat a fogyasztókkal, kialakítja az árakat, megszervezi az értékesítést és befolyásolja a vásárlókat". Kiterjesztett értelemben azonban „a marketing minden értékkel rendelkező jószág (termék, szolgáltatás, eszme, ötlet, érzés stb.) cseréje. Az üzleti, vállalati szférán túl kiterjed az olyan nem nyereségorientált területekre is, mint például az oktatás, a kultúra, a vallás, a politika stb." [28: 1.1.1., 1.1.3.].

Mint látható, a marketing nem csupán termékek és szolgáltatások, hanem lényegében bármilyen gondolat, eszme, sőt akár személy megismertetését, elfogadtatását és népszerűsítését is szolgálhatja. Ebben az értelemben a biztonságtudatosítás területén is alkalmazható a marketing fogalma, ahol a szervezet a biztonságtudatosság értékét közvetíti a „vevők", azaz az alkalmazottak felé, és sikeres „értékesítés" esetén a munkatársak megfelelő biztonságtudatossága lesz az eredmény.

A marketing egyik legfontosabb eszköze a marketingkommunikáció, ami olyan tervezett cselekvéssorozat, amely a vállalat marketingrendszerébe illeszkedik, célja egy termék (szolgáltatás), márka vagy vállalat (intézmény) megismertetése, népszerűsítése, a fogyasztó figyelmének felkeltése, vásárlásra ösztönzése, illetve érdeklődésének megtartása kommunikáció segítségével [29: 12.]. Az ismertetett célrendszer teljes egészében megfeleltethető a biztonságtudatosítási program céljainak, sőt, a jelenleg alkalmazott programok alapvető célkitűzéseit meg is haladja, amennyiben beépíti új elemként az érdeklődés folyamatos fenntartását kommunikációs eszközök segítségével. Ezért érdemes áttekinteni, hogy a marketingkommunikáció eszközei közül melyik adoptálható és alkalmazható a biztonságtudatosítási programok megvalósítása során.

A marketingkommunikáció eszközei közül van egy kifejezetten olyan terület, amely dedikáltan a vállalaton belüli kommunikációval foglalkozik, ez pedig a belső PR (public relations). „A belső, vagy más néven vállalati PR esetében a vállalat beosztottjai és vezetői között zajlik a kommunikáció, az információáramlás. Ennek az a fő célja, hogy a dolgozók minél jobban megismerjék a cégük (munkahelyük) céljait, azzal tudjanak azonosulni, és azokat a saját maguk által alkalmazható megfelelő eszközökkel tudják elősegíteni" [30: 36.].

A tudatosítási program sikere szempontjából kiemelkedő jelentőséggel bír, hogy a résztvevők el tudják-e fogadni és elismerik-e az információbiztonság szervezeti jelentőségét, képesek-e a magatartásukat, mindennapi tevékenységüket ennek megfelelően alakítani és ezzel a szervezet hosszú távú célját, a biztonságtudatos szervezeti kultúra kialakítását támogatni.

Éppen ezért vizsgáljuk meg, hogy a belső PR eszközei alkalmazhatók-e, és ha igen, milyen formában a biztonságtudatosítási programban.

A könnyebb áttekinthetőség érdekében a belső PR három csoportba sorolt [30: 39–40.], azaz a személyes, a csoportkommunikációs és a tömegkommunikációs eszközei közül

a számunkra releváns elemeket és azok lehetséges alkalmazási területeit az alábbi táblázatban foglaltam össze.

1. táblázat

A belső PR eszközeinek lehetséges alkalmazási területei a biztonságtudatosító programban
[a szerző szerkesztése]

Belső PR eszközei	Biztonságtudatosító program
1. A személyes kommunikáció eszközei	*1. A személyes kommunikáció eszközei*
Párbeszéd, megbeszélés	Az információbiztonsági incidens által érintett vagy érintettek személyes megkeresése, a problémák okának feltárása, megoldási javaslatok közös kidolgozása, visszaellenőrzés.
Előadás	Előadások tartása a felhasználók számára az információbiztonság egy-egy, ugyanakkor mindenkit érintő kérdéséről.
Telefonbeszélgetés	Az információbiztonsági problémával, kérdéssel a szakterülethez fordulók telefonon történő tájékoztatása a teendőkről, a felmerülő kérdések átbeszélése, visszaellenőrzés.
Levelezés, e-mailek	Az információbiztonsági problémával, kérdéssel a szakterülethez fordulók e-mail útján történő tájékoztatása a teendőkről, a felmerülő kérdések átbeszélése, visszaellenőrzés.
Meghívók	Meghívók küldése akár nyomtatva, akár online egy-egy rendezvényre, megbeszélésre, előadásra, amelynek célja a figyelem felkeltése a program iránt.
Oklevelek	Motivációs eszközként, például interaktív játékban történő részvételért, egy incidens kezelésében nyújtott segítő közreműködésért, információbiztonsági kvízek eredményes kitöltéséért.
2. A csoportkommunikáció eszközei	*2. A csoportkommunikáció eszközei*
Konferencia típusú rendezvények [31: 17.]	Például: • **tájékoztatók** egy-egy, a legtöbb munkatársat érintő incidens esetén; • **tematikus konferenciák/fórumok**, például szakértők meghívása social engineering témában; • **értekezletek** egy incidens kapcsán az érintetti körrel; • **képzések, továbbképzések** szervezése például vezetői körnek, átlagfelhasználóknak; • több telephellyel rendelkező szervezetek esetén **road-show** alkalmazása.
Audiovizuális PR-eszközök, mint • Diaképek, írásvetítő fóliák, szemléltetőeszközök • PR-filmek, videók • Multimédia • Számítógépes prezentáció • Computer-animáció	**Audiovizuális eszközöket** szemléltetés céljából nagyon fontos alkalmazni a konferenciatípusú rendezvényeken, de személyes megbeszélések vagy értekezletek alkalmával is, akár prezentáció, akár képek, videóanyagok vagy egyéb eszközök formájában. A **PR-filmek és -videók** nemcsak konferenciatípusú rendezvényen alkalmazhatók, hanem például az intraneten is közzé lehet tenni, vagy körlevélben elküldeni. Ezek a figyelemfelhívó videók általában 1-5 perc hosszú, dramatizált filmanyagok, amelyek egy biztonsági kockázatot vagy annak helyes kezelését mutatják be [32], vagy például a saferinternet.hu weboldalon számos a gyermekeknek, fiataloknak és szülőknek, pedagógusoknak szóló videó található [33].

Belső PR eszközei	Biztonságtudatosító program
Hagyományos nyomtatványok	Bár egyre kevésbé használatos, de még mindig találkozhatunk a hagyományos nyomtatványokkal, mint például • a **vállalati/szervezeti újság**, amelybe egy-egy az információbiztonsággal kapcsolatos érdekesség, fontos hír is helyet kaphat, • konferencia, szakmai fórum **meghívók,** • **tájékoztató kiadványok** az információbiztonság egy-egy kérdéséről, • **szervezeti éves/féléves/negyedéves beszámolóban** az információbiztonságot érintő statisztikák, tapasztalatok bemutatása, • faliújságon figyelemfelkeltő **poszterek, plakátok** elhelyezése, vagy egy-egy **program hirdetése.**
Hírlevelek, (News Release)	**Hírlevelek**, vagy **professzionálisan megírt cikkek nyomtatott vagy online verzióban.** Lényege, hogy könnyen áttekinthető és könnyen olvasható legyen. Hírlevél keretében tájékoztatni tudjuk a munkatársakat **egy rendkívüli esemény kiértékelését követően a következtetésekről.**
Aktuális cikkajánlások	**Magyar vagy a nemzetközi sajtóból egy-egy érdekes cikk** ajánlása tipikusan online formában.
Faliújságok, hirdetések	A **belső intranethálózaton** figyelemfelkeltő **poszterek** elhelyezése, egy-egy program **hirdetése**, vagy **tudatosító kiadványok** népszerűsítése, **tájékoztató honlapok** elérési útvonalának megosztása (például EU, ENISA aktuális döntései, kiadványai).
3. A tömegkommunikáció eszközei	*3. A tömegkommunikáció eszközei*
Online magazinok, portáloldalak	Körlevélben vagy az intraneten érdemes megosztani azon oldalak elérhetőségét, amelyek naprakész információkat, figyelemfelhívó módon, röviden összefoglalva osztanak meg az érdeklődőkkel (például a Nemzeti Kibervédelmi Intézet hírlevele [34]).
Online kapcsolatok: fórum, hírlevél, levelezőlista	**Internetes csevegőfórumok, közösségi felületek**

Az internetes csevegőfórumok, közösségi felületek kapcsán külön szeretnék kitérni néhány mondat erejéig a Nemzeti Közszolgálati Egyetem (NKE) várhatóan 2019 decemberében induló pilot programjára. Az NKE által üzemeltetett Továbbképzési és Vizsgaportálon, az úgynevezett Probono oldalon egy olyan információbiztonság-tudatosító tesztcsatornát fejlesztettek ki, amely egy Facebookhoz hasonló közösségi oldal, amelynek célja, hogy egyszerű, rövid, a napi gyakorlatban és a munkavégzés során jól alkalmazható tudást közvetítsen az érdeklődők felé érdekes, újszerű formában. Három, az IT és információbiztonság terén jártas szakértő közreműködésével a hét minden napján új tartalommal jelentkezik a portál hol hosszabb, tartalmasabb cikkek, hol pedig rövidebb bejegyzések, képek/poszterek, a nemzetközi, illetve a magyar sajtóban megjelent, általuk kommentált hírek formájában.

A csatornára feliratkozóknak lehetőségük van hozzászólni a közzétett bejegyzésekhez, kérdezni és segítséget kérni a szakértőktől, vagy esetleg egy általuk fontosnak tartott témát javasolni későbbi feldolgozásra.

A csatorna jelenleg tesztelés alatt áll, de reményeink szerint az információbiztonság-tudatosítás egy teljesen újszerű és minden eddiginél hatékonyabb, a résztvevők saját belső motivációjára építő önfejlesztési formát biztosít a közszolgálatban dolgozóknak.

A táblázatban felsorolt eszközök, módszerek kiválóan alkalmazhatók a tudatosítási programok megvalósítása során, sőt, egy részüket jelenleg is alkalmazzák a szervezetek, ugyan nem tudatosan és kimondottan marketingkommunikációs eszközként.

Az összehasonlítással azonosítottam azokat a belső PR-eszközöket, amelyek adaptálhatók egy tudatosítási programba, és meghatároztam az adott eszközök alkalmazási területeit és formáit is, példákkal alátámasztva. Célom egy olyan módszertani gyűjtemény létrehozása volt, amelynek segítségével egyrészt hatékonyabban tudja a vezetés az információbiztonság értékét eljuttatni a munkatársakhoz, másrészt a szervezetek – figyelembe véve a sajátosságaikat, a célcsoportot és az átadni kívánt ismereteket –, össze tudnak állítani egy hatékony tudatosítási programot.

Tehát a felsorolt eszközök csupán egy összefoglalása az alkalmazható módszerek sokszínűségének, minden szervezetnek magának kell az eszközök megfelelő kombinációjával biztosítania a tudatosítási programjuk sikerességét.

3.3. Az időzítés megtervezése

Nagyon fontos, hogy a tudatosítási program keretében a munkavállalók ne csak egyetlen egyszer találkozzanak az információbiztonsággal, például egy hagyományos frontális képzés keretében, amikor belépnek a szervezethez, hanem gondosan megtervezett tudatosító program keretében, meghatározott időközönként valamilyen formában találkozzanak az információbiztonsággal. Ahogy a mondás is tartja, „ismétlés a tudás anyja." A tapasztalatok azt mutatják, hogy ha abbahagyjuk a tanulást, akkor a megszerzett ismeretanyag és tudás szintje exponenciálisan elkezd csökkenni, éppen ezért nagyon fontos az élethosszig tartó tanulás. Minél többet olvasunk és tanulunk, minél nagyobb a tudásunk, annál nagyobb eséllyel hívjuk elő az adott helyzetben szükséges információkat. És ez igaz az információbiztonság-tudatosító programokra is. Egyrészt ezért is nagyon fontos, hogy rendszeresen közvetítsünk új és ismételt információkat, illetve tudásanyagot a munkatársak felé, másrészt azért is, mert a támadók folyamatosan újabb és újabb típusú támadás megvalósításán kísérleteznek, ezért nagyon fontos az információbiztonsággal kapcsolatos ismeretek naprakészen tartása.

Következtetések

A közigazgatás digitális átalakításának, az e-közigazgatás megteremtésének köszönhetően, mára már a nemzeti adatvagyon jelentős részét elektronikus információs rendszerekben tárolják, amelyeket az arra kötelezett szervek a legmodernebb fizikai és logikai védelmi intézkedésekkel és technológiai megoldásokkal védik az illetéktelen személyekkel és a lehetséges támadásokkal szemben. Éppen ezért a támadók azt a pontját támadják egy rendszernek, amely a leggyengébbnek bizonyul, ez pedig nem más, mint az ember. Bárhogy is védjük rendszereinket, mind hiábavaló, ha munkatársaink figyelmetlenségből, hanyagságból vagy netán rosszindulatból, vagy egyszerűen csak az alapvető informatikai és elektronikus információbiztonsági ismeretek hiányából

fakadóan nem tudnak, vagy nem akarnak biztonságtudatosan és felelősségteljesen viselkedni rendszereik és eszközeik (például okostelefon, pendrive) használatakor.

A hatékony és eredményes kiberbiztonság és a biztonságtudatos szervezeti kultúra megteremtésének az egyik legfontosabb eleme a közszférában dolgozók megfelelő felkészültsége, a biztonságtudatosság, aminek kialakításához sikeres és hatékony biztonságtudatosítási program megszervezése és folyamatos fenntartása, menedzselése szükséges.

Tanulmányommal segítséget kívánok nyújtani egy olyan tudatosítási program kidolgozásához, amely képes a felhasználók biztonságtudatosságát növelni. Ennek érdekében megvizsgáltam a biztonságtudatosság fogalmi összetevőit és megállapítottam, hogy ez nemcsak az informatikai és információbiztonsági ismeretekre épül, hanem nélkülözhetetlen elemei a fenyegetések korai felismerését és a reagálást biztosító képességek és az információbiztonság jelentőségét hangsúlyozó magatartás is. E három fontos területet fejlesztő tudatosítási program kidolgozása érdekében tanulmányoztam a programok lényegi elemeit, a cél- és eszközrendszerét vizsgáló nemzetközi kutatásokat, és arra a következtetésre jutottam, hogy csak akkor biztosítható a sikeresség, ha beazonosítjuk a program célcsoportját és annak biztonságtudatossági szintjét (Kinek?), specifikusan meghatározzuk a nekik megfelelő ismereteket (Mit?), és ezeket a célcsoporthoz, valamint a szervezethez illeszkedő kommunikációs csatornák és eszközök segítségével közvetítjük feléjük (Hogyan?). A megfelelő közvetítő közeg biztosítása érdekében megvizsgáltam, hogy a marketingkommunikáció és azon belül a belső PR fogalma és eszközrendszere alkalmazható-e a biztonságtudatossági programra. Arra a megállapításra jutottam, hogy a belső PR-nak számos olyan személyes, csoportos és tömegkommunikációs eszköze, módszere van, amely sikeresen alkalmazható a tudatosítási programok során, sőt, néhányat már a szervezetek alkalmaznak is.

Tanulmányom legfontosabb következtetése, hogy a tudatosítási programok tekintetében nem határozható meg egy minden szervezetre érvényes megoldási javaslat, amely hatékonysághoz és sikerességhez vezet, minden szervezetnek a maga sajátosságaihoz és igényeihez igazodó, valamint változatos kommunikációs csatornákat és eszközöket alkalmazó tudatosítási programot kell kidolgoznia és megvalósítania.

Hivatkozások

[1] „A Digitális Jólét Program 2.0," *digitalisjoletprogram.hu,* 2017. július. [Online]. Elérhető: https://digitalisjoletprogram.hu/files/57/1c/571c60381c274901733f8a2fc8a1cca5.pdf (Letöltve: 2019. 10. 27.)

[2] Cs. Krasznay, „A polgárok védelme egy kiberkonfliktusban," *Hadmérnök,* 7. évf. 4. sz., pp. 142–151., 2012.

[3] NTT Security, "Global Threat Intelligence Report." *NTT Security,* 2019, [Online]. Elérhető: www.nttsecurity.com/docs/librariesprovider3/resources/2019-gtir/2019_gtir_report_2019_uea_v2.pdf (Letöltve: 2019. 11. 15.)

[4] A. Beláz, „A közigazgatás információbiztonsága: megjósolhatók az incidensek?," *Hadtudomány: A magyar Hadtudományi Társaság folyóirata,* 29. évf. 3. sz., pp. 92–104., 2019. DOI: https://doi.org/10.17047/HADTUD.2019.29.3.92
[5] I. Legárdné Nagy, A biztonságos számítógép-használat jogi és szabályozási háttere – Az elektronikus információbiztonság-tudatosság és tudatosítás jelenlegi helyzete, lehetőségei és kihívásai a közszolgálatban, Diplomamunka, Nemzeti Közszolgálati Egyetem, Budapest, 2018.
[6] V. Deák, „A social engineering humán alapú támadási technikái," *Biztonságpolitika.hu,* p. 11, 2017. április 10.
[7] P. Bányász, „Social engineering and social media," *Nemzetbiztonsági Szemle,* 6. évf. 1. sz., pp. 59–77., 2018.
[8] V. Deák, „A számítógép alapú social engineer támadási technikák," *Biztonságpolitika.hu,* 2017. április 28.
[9] L. Muha és Cs. Krasznay, *Az elektronikus információs rendszerek biztonságának menedzselése.* Budapest: Nemzeti Közszolgálati Egyetem Vezető- és Továbbképzési Intézet, 2014.
[10] V. Deák, „A nyílt forrású információszerzés szerepe a kibertámadások végrehajtása során," *Hadmérnök,* 13. évf. *3. sz.,* pp. 391–402., 2018.
[11] V. Deák, „Kártékony programok terjedése social engineering technikákon keresztül," *Hadmérnök,* 14. évf. 2. sz., pp. 256–271., 2019.
[12] I. Veseli, *Measuring the Effectiveness of Information Security Awereness Program.* M. S. thesis, Gjøvik University College, Gjøvik, 2011, p. 87.
[13] R. S. Shaw, C. C. Chen, A. L. Harris and H.-J. Huang, "The impact of information richness on information security awareness training effectiveness," *Computers & Education,* vol. 52, no. 1, pp. 92–100, Jan. 2009. DOI: https://doi.org/10.1016/j.compedu.2008.06.011
[14] H. Aldawood and G. Skinner, "Reviewing Cyber Security Social Engineering Training and Awareness Programs – Pitfalls and Ongoing Issues," *Future Internet,* vol. 11, no. 3. p. 73, 2019. DOI: https://doi.org/10.3390/fi11030073
[15] A. Nemeslaki és P. Sasvári, „Az információbiztonság-tudatosság empirikus vizsgálata a magyar üzleti és közszférában," *Infokommunikáció és Jog,* 60. sz., pp. 169–177., 2014.
[16] B. Bulgurcu, H. Cavusoglu and I. Benbasat, "2010: Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly,* vol. 34, no. 3, pp. 523–548, 2010. DOI: https://doi.org/10.2307/25750690
[17] M. Illésy, A. Nemeslaki és Z. Som, „Elektronikus információbiztonság-tudatosság a magyar közigazgatásban," *Információs Társadalom,* 14. évf. 1. sz., pp. 52–73., 2014.
[18] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról
[19] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
[20] 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott techno-

lógiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről
[21] L. Nagy, „Az informatikai kultúra – különös tekintettel a felhasználói tudatosságra – a Magyar Honvédség szervezetében a generációk viszonyrendszerében," *Hadtudományi Szemle,* 8. évf. 4. sz., pp. 393–431., 2015.
[22] A. Schüller, „Az Y generáció és az információbiztonság," *Hadmérnök,* 6. évf. 2. sz., pp. 339–347., 2011.
[23] M. Bada, A. M. Sasse and J. R. C. Nurse, "Cyber Security Awareness Campaigns: Why do they fail to change behaviour?," Jan. 2015. [Online]. Elérhető: https://arxiv.org/ftp/arxiv/papers/1901/1901.02672.pdf (Letöltve: 2019. 10. 29.)
[24] A. N. W Prah, A. A. Otchere and K. E. Opan, "The perceived effectiveness of information security awareness," *Information and Knowledge Management,* vol. 6, no. 7, p. 62, 2016.
[25] Cs. Kollár, „Az információbiztonság-tudatosság fejlesztése a (felső)vezetők körében coaching és tanácsadás módszerével," *Magyar Coachszemle,* 5. évf. 3. sz., pp. 35–50., 2016.
[26] A. Szász és G. Kiss, „Jelszóvisszafejtő programok oktatási célú felhasználása és hatásuk az információbiztonsági tudatosságra," *Információs Társadalom,* 18. évf. 3–4. sz., pp. 82–104., 2018. DOI: https://doi.org/10.22503/inftars.XVIII.2018.3-4.4
[27] „Security Awareness Report," *naganresearchgroup.com,* 2017, [Online]. Elérhető: www.naganresearchgroup.com/SANSSAR2017.pdf (Letöltve: 2019. 11. 02.)
[28] A. Bauer és J. Berács, *Marketing.* Budapest: Akadémia Kiadó, 2016. DOI: https://doi.org/10.1556/9789634540076
[29] I. Fazekas és D. Harsányi, *Marketingkommunikáció érthetően.* Budapest: Szókratész Külgazdasági Akadémia, 2011.
[30] E. Lendvai és J. Gál, *Marketingkommunikáció 1.* Budapest: TÁMOP-4.1.2-08/1/A, Új Magyarország Fejlesztési Terv, 2011. [Online]. Elérhető: https://regi.tankonyvtar.hu/hu/tartalom/tamop425/0034_marketingkomm_1/adatok.html (Letöltve: 2019. 10. 28.)
[31] H. Csáfor, *Vállalatok külső és belső kommunikációja (PR).* Eger: Eszterházy Károly Főiskola, 2012.
[32] Youtube, „60 másodperc biztonság – Az internet veszélyei," *Youtube,* [Online]. Elérhető: www.youtube.com/watch?v=ISPAFbkh424. (Letöltve: 2019. 11. 03.)
[33] Safer internet, „Biztonságosabb internet pedagógusoknak," *Safer internet,* [Online]. Elérhető: http://saferinternet.hu/tippek-videok/szuloknek-pedagogusoknak (Letöltve: 2019. 11. 03.)
[34] „eGov hírlevél," [Online]. Elérhető: https://hirlevel.egov.hu/tag/nemzeti-kibervedelmi-intezet/ (Letöltve: 2019. 11. 03.)